SwA as a Critical Component of Cybersecurity

Andy Purdy
Chief Cybersecurity Strategist
CSC

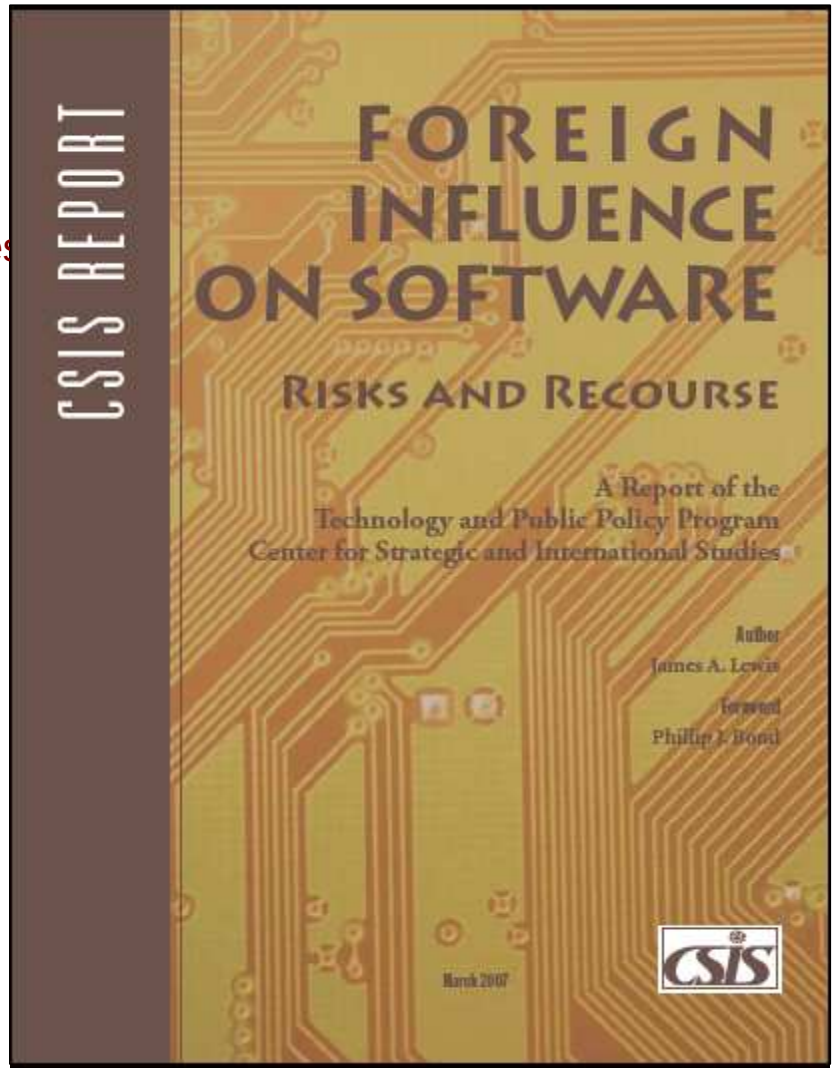
SwA Forum

March 12, 2010

Recommendations Addressing Globalization of Software

Center for Strategic and International Studies Report on Risks and Recourse

1. Assess risk (and share assessment)
2. Focus on assurance, not location
3. Avoid one-size-fits-all solutions
4. Refocus and reform existing certification processes
5. Identify commercial best practices and tools and expand their use
6. Create governance structure(s) for assurance
7. Accelerate info assurance efforts
8. Promote leadership in IT innovation



March 2007 Report CSIS

Recommendations Addressing Globalization of Software

Defense Science Board Task Force September 2007 Report on "Mission Impact of Foreign Influence on DoD Software"

Findings relate to:

- -The Industry Situation
- -Dependence on Software-
- -Software Vulnerabilities
- -Threat of the Nation-State Adversary
- -Awareness of Software Assurance Threat and Risk
- -Status of Software Assurance
- -Ongoing Efforts in Software Assurance
- -Supplier Trustworthiness Considerations
- -Finding Malicious Code
- -Government Access to Source Code

Recommendations relate to:

- -Procurement of COTS and Off-Shore Software
- -Increase US Insight into Capabilities and Intentions
- -Offensive Strategies can complicate Defensive Strategie
- -System Engineering and Architecture for Assurance
- -Improve the Quality of Software
- -Improve Tools and Technology for Assurance
- -More Knowledgeable Acquisition of Software
- -Research and Development in Software Assurance

Eliminate excess functionality in mission-critical components

Improve effectiveness of Common Criteria

Improve usefulness of assurance metrics

Promote use of automated tools in development

Increase transparency and knowledge of suppliers' processes

Components should be supplied by suppliers of commensurate trustworthiness

Custom code for critical systems should be developed by cleared US citizens

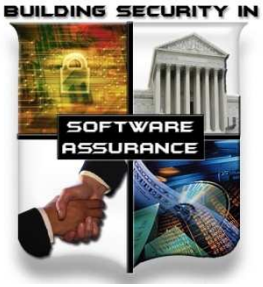
Provide incentives to industry to produce higher quality code; improve assuredness of COTS SW

Use risk-based acquisition

Research programs to advance vulnerability detection and mitigation

Advance the issue of software assurance and globalization on national agenda as part of effort to reduce national cyber risk

Assurance Challenges in Mitigating Software Supply Chain Risks



- Complexity hampers our ability to determine and predict code behavior; so any "assurance" claims for security/safety-critical applications are limited.
- Without adequate diagnostic capabilities and commonly recognized standards from which to assert claims about the assurance of products, systems and services, the "providence and pedigree of supply chain actors" become a more dominant consideration for security/safety-critical applications:
  - Consumers lack requisite transparency for more informed decision-making for mitigating risks;
  - Favoring domestic suppliers does not necessarily address 'assurance' in terms of capabilities to deliver secure/safe components.
- Several needs arise:
  - **Need internationally recognized standards** to support processes and provide transparency for more informed decision-making for mitigating enterprise risks.
  - **Need 'Assurance' to be explicitly addressed in standards & capability benchmarking models** for organizations involved with security/safety-critical applications.
  - **Need more comprehensive diagnostic capabilities** to provide sufficient evidence that "code behavior" can be well understood to not possess exploitable or malicious constructs.

DHS NCSD Software Assurance (SwA) Program

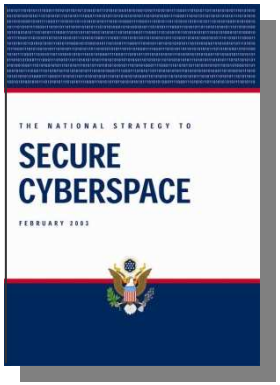
Through public-private collaboration promotes security and resilience of software throughout the lifecycle; focused on reducing exploitable software weaknesses and addressing means to improve capabilities that routinely develop, acquire, and deploy resilient software products.

- **Serves as a *focal point* for interagency public-private collaboration to enhance development and acquisition processes and capability benchmarking to address software security needs.**
  - Hosts interagency Software Assurance Forums, Working Groups and training to provide public-private collaboration in advancing software security and providing publicly available resources.
  - Provides collaboratively developed, peer-reviewed information resources on Software Assurance, via journals, guides & on-line resources suitable for use in education, training, and process improvement.
  - Provides input and criteria for leveraging international standards and maturity models used for process improvement and capability benchmarking of software suppliers and acquisition organizations.
- ***Enables software security automation and measurement capabilities* through use of common indexing and reporting capabilities for malware, exploitable software weaknesses, and common attacks which target software.**
  - Collaborates with the National Institute of Standards and Technology, international standards organizations, and tool vendors to create standards, metrics and certification mechanisms from which tools can be qualified for software security verification.
  - Manages programs to facilitate the adoption of Malware Attribute Enumeration Classification (MAEC), Common Weakness Enumeration (CWE), and Common Attack Pattern Enumeration and Classification (CAPEC).

DHS Software Assurance Program Overview

- Program established in response to the National Strategy to Secure Cyberspace - Action/Recommendation 2-14:

  "DHS will facilitate a national public-private effort to promulgate best practices and methodologies that promote integrity, security, and reliability in software code development, including processes and procedures that diminish the possibilities of erroneous code, malicious code, or trap doors that could be introduced during development."



- DHS Program goals promote the **security and resilience** of software across the development, acquisition, and operational life cycle
- DHS Software Assurance (SwA) program is scoped to address:
  - **Trustworthiness** - No exploitable vulnerabilities or malicious logic exist in the software, either intentionally or unintentionally inserted,
  - **Dependability (Correct and Predictable Execution)** - Justifiable confidence that software, when executed, functions as intended,
  - **Survivability** - If compromised, damage to the software will be minimized, and it will recover quickly to an acceptable level of operating capacity;
  - **Conformance** – Planned, systematic set of multi-disciplinary activities that ensure processes/products conform to requirements, standards/procedures.

DHS Software Assurance Program Structure *

- As part of the DHS risk mitigation effort, the SwA Program seeks to reduce software vulnerabilities, minimize exploitation, and address ways to improve the routine development of trustworthy software products and tools to analyze systems for hidden vulnerabilities.
- The SwA framework encourages the production, evaluation and acquisition of better quality and more secure software; leverages resources to target the following four areas:
  - education and training for developers and users
  - sound practices, standards, and practical guidelines for the development of secure software
  - diagnostic tools, cyber security R&D and measurement
  - due-diligence questionnaires, contract templates and guidelines for acquisition management and outsourcing

* July 28, 2006 statement of George Foresman, DHS UnderSecretary for Preparedness, before the U.S. Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Federal Financial Management, Government Information, and International Security

Software Assurance "End State" Objectives…

- **Government, in collaboration with industry / academia, *raised expectations* for product assurance with requisite levels of integrity and security:**
  - Helped advance more comprehensive software assurance diagnostic capabilities to mitigate risks stemming from exploitable vulnerabilities and weaknesses;
  - Collaboratively advanced use of software security measurement & benchmarking schemes
  - Promoted use of methodologies and tools that enabled security to be part of normal business.
- **Acquisition managers & users factored risks posed by the software supply chain as part of the trade-space in risk mitigation efforts:**
  - Information on suppliers' process capabilities (business practices) would be used to determine security risks posed by the suppliers' products and services to the acquisition project and to the operations enabled by the software.
  - Information about evaluated products would be available, along with responsive provisions for discovering exploitable vulnerabilities, and products would be securely configured in use.
- **Suppliers with requisite integrity and made assurance claims about the IT/software safety, security and dependability:**
  - Relevant standards would be used from which to base business practices & make claims;
  - Qualified tools used in software lifecycle enabled developers/testers to mitigate security risks;
  - Standards and qualified tools would be used to certify software by independent third parties;
  - IT/software workforce had requisite knowledge/skills for developing secure, quality products.

Going Forward

- Knowledge and technology transfer
  - Website, pocket guides, training, outreach
  - Consulting
  - Resources
  - Government
  - NCSD, FNS
  - DHS/OMB requirements
  - Driving progress so SwA becomes real
  - Standards
  - Acquisition (FAR)(streamline)
  - Education (SWA requirements for COEs)
  - Adoption

Contact Information

Andy Purdy

Chief Cybersecurity Strategist

CSC

dpurdy@csc.com

703-641-2176